

Week 11: Final Cloud Security Audit

Name- Samruddhi Dattu Nikam

PRN- 2124UCF2019

Email- samruddhi.nikam_24ucs@sanjivani.edu.in

- Tasks-**
- 1) Review all resources.
 - 2) Identify misconfigurations.
 - 3) Document final audit report.

Task 1- Review All Resources.

EC2 Instances:



| Security group ID | Security group name | VPC ID | Description | QoS |
|----------------------|---------------------|----------------------|----------------------------|-----|
| sg-0a2677257fd4d8378 | security_group | vpc-04d890dc91357448 | first security group | 24 |
| sg-0dx1267f966b37428 | default | vpc-04d890dc91357448 | default VPC security group | 24 |

S3 Buckets:



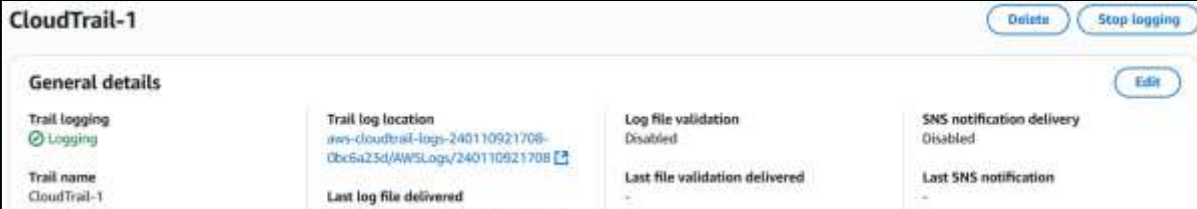
| Objects | Properties | Permissions | Metrics | Management | Access Points |
|--|------------|---|---------|--|---------------|
| Bucket overview | | | | | |
| AWS Region Asia Pacific (Mumbai) ap-south-1 | | Amazon Resource Name (ARN) arn:aws:s3:::2124ucsm2011 | | Creation date July 17, 2025, 22:29:20 (UTC+05:30) | |

IAM Users/Roles:



| IAM resources | | | | |
|-------------------------------|-------|-------|----------|--------------------|
| Resources in this AWS Account | | | | |
| User groups | Users | Roles | Policies | Identity providers |
| 1 | 2 | 27 | 0 | 0 |

CloudTrail & Config:



| General details | | | |
|----------------------------|--|-------------------------------------|---------------------------------------|
| Trail logging Logging | Trail log location aws-cloudtrail-logs-240110921708-0bc6a25d/AWSLogs/240110921708 | Log file validation Disabled | SNS notification delivery Disabled |
| Trail name CloudTrail-1 | Last log file delivered August 18, 2025, 18:47:57 (UTC+05:30) | Last file validation delivered - | Last SNS notification - |

Task 2- Identify Misconfigurations.

S3 Buckets:

do-not-delete-ssm-diagnosis-240110921708-ap-south-1-dfbay

Objects

Properties

Permissions

Metrics

Management

Access Points

Bucket overview

AWS Region

Asia Pacific (Mumbai) ap-south-1

Amazon Resource Name (ARN)

arn:aws:s3::do-not-delete-ssm-diagnosis-240110921708-ap-south-1-dfbay

Creation date

July 27, 2025, 17:54:21 (UTC+05:30)

IAM:

compromised-user

Info

Delete

Summary

ARN

arn:aws:iam::240110921708:user/compromised-user

Console access

Disabled

Access key 1

Create access key

Created

August 18, 2025, 13:09 (UTC+05:30)

Last console sign-in

-

CloudTrail:

CloudTrail-1

Delete

Stop logging

General details

Edit

Trail logging

Logging

Trail name

CloudTrail-1

Multi-region trail

Yes

Apply trail to my organization

Not enabled

Trail log location

aws-cloudtrail-logs-240110921708-0bc6a25d/AWSLogs/240110921708

Last log file delivered

August 18, 2025, 20:03:42 (UTC+05:30)

Log file SSE-KMS encryption

Not enabled

Log file validation

Disabled

Last file validation delivered

-

SNS notification delivery

Disabled

Last SNS notification

-